AMENDMENTS

In the Claims:

This listing of claims will replace all prior versions or listings of claims for this application.

1-8. (Cancelled).

9. (Currently amended) A method for selecting a digital object in a database, the method comprising:

generating a plurality of encryption keys, each encryption key associated with one of a plurality of digital objects stored in an electronic database;

encrypting the plurality of digital objects using the associated encryption keys;

encrypting the plurality of encryption keys ~~using a first cryptography scheme~~ by the database;

transmitting to a requester the plurality of encrypted digital objects and encryption keys;

receiving from the requester at least one of the encryption keys, wherein the received encryption key has been ~~further encrypted using a second cryptography scheme~~ re-encrypted by the requester prior to transmission;

generating a partially decrypted encryption key at the database by decrypting the received encryption key ~~using the first cryptography scheme~~; and

transmitting the partially decrypted encryption key to the requester.

10. (Previously Presented) The method of claim 9, further comprising encrypting the plurality of encryption keys by determining $(\text{encryption key})^{(\text{random number R})}$ mod (prime number p) for each key.

11. (Currently amended) The method of claim 9, further comprising decrypting the received encryption key by determining ~~(encryption key)$^{(1/(\text{random number R}) \bmod (\text{prime number p} - 1))}$ mod (prime number p)~~ (encryption key)$^{(1/(\text{random number R}) \bmod (\text{prime number p}) - 1)}$ mod (prime number p).

12. (Previously presented) The method of claim 10, further comprising performing the modulo operation if computation of a discrete logarithm is not possible.

13. (Currently amended) A method for selecting a digital object in a database, the method comprising:

requesting a plurality of digital objects from an electronic database;

receiving from the database the requested plurality of digital objects, wherein each digital object has been encrypted using an associated encryption key;

receiving from the database the plurality of keys associated with the plurality of digital objects wherein each key has been encrypted ~~using a first cryptography scheme~~ by the database;

selecting a ciphertext key from the plurality of received keys;

~~further encrypting~~ re-encrypting the selected key ~~using a second cryptography scheme~~;

transmitting the key to the database;

receiving from the database the key wherein the key has been partially decrypted ~~using the first cryptography scheme~~ by the database;

decrypting the partially decrypted key ~~using the second cryptography scheme~~ to generate a decrypted key; and

decrypting the received digital object using the decrypted key.

14. (Previously Presented) The method of claim 13, further comprising encrypting the plurality of encryption keys by determining (encryption key)$^{(\text{random number R})}$ mod (prime number p) for each key.

15. (Currently amended) The method of claim 13, further comprising decrypting the received encryption key by determining ~~(encryption key)$^{(1/(\text{random number R}) \bmod (\text{prime number p} - 1))}$ mod (prime number p)~~ (encryption key)$^{(1/(\text{random number R}) \bmod (\text{prime number p}) - 1)}$ mod (prime number p).

16. (Previously presented) The method of claim 14, further comprising performing the modulo operation if computation of a discrete logarithm is not possible.

17. (Currently amended) A system for selecting a digital object in a database, the system comprising a processor for:

generating a plurality of encryption keys, each encryption key associated with one of a plurality of digital objects stored in an electronic database;

encrypting the plurality of digital objects using the associated encryption keys;

encrypting the plurality of encryption keys ~~using a first cryptography scheme~~ by the database;

transmitting to a requester the plurality of encrypted digital objects and encryption keys;

receiving from the requester at least one of the encryption keys, wherein the received encryption key has been ~~further encrypted using a second cryptography scheme~~ re-encrypted;

generating a partially decrypted encryption key at the database by decrypting the received encryption key ~~using the first cryptography scheme~~; and

transmitting the partially decrypted encryption key to the requester.

18. (Previously Presented) The system of claim 17, wherein the processor is further configured or arranged for encrypting the plurality of encryption keys by determining (encryption key)$^{(\text{random number R})}$ mod (prime number p) for each key.

19. (Currently amended) The system of claim 17, wherein the processor is further configured or arranged for decrypting the received encryption key by determining ~~(encryption key)$^{(1/(\text{random number R}) \bmod (\text{prime number p} - 1))}$ mod (prime number p)~~ (encryption key)$^{(1/(\text{random number R}) \bmod (\text{prime number p}) - 1)}$ mod (prime number p).

20. (Previously presented) The system of claim 18, wherein the processor is further configured or arranged for performing the modulo operation if computation of a discrete logarithm is not possible.

21. (Currently amended) A system for selecting a digital object in a database, the system comprising a processor for:

requesting a plurality of digital objects from an electronic database;

receiving from the database the requested plurality of digital objects, wherein each digital object has been encrypted using an associated encryption key;

receiving from the database the plurality of keys associated with the plurality of digital objects wherein each key has been encrypted ~~using a first cryptography scheme~~ by the database;

selecting a ciphertext key from the plurality of received keys;

~~further encrypting~~ re-encrypting the selected key ~~using a second cryptography scheme~~;

transmitting the further key to the database;

receiving from the database the key wherein the key has been partially decrypted ~~using the first cryptography scheme~~ by the database;

decrypting the partially decrypted key ~~using the second cryptography scheme~~ to generate a decrypted key; and

decrypting the received digital object using the decrypted key.

22. (Previously Presented) The system of claim 21, wherein the processor is further configured or arranged for encrypting the plurality of encryption keys by determining (encryption key)$^{(\text{random number R})}$ mod (prime number p) for each key.

23. (Currently amended) The system of claim 21, wherein the processor is further configured or arranged for decrypting the received encryption key by determining ~~(encryption key)$^{(1/(\text{random number R}) \bmod (\text{prime number p} - 1))}$ mod (prime number p)~~ (encryption key)$^{(1/(\text{random number R}) \bmod (\text{prime number p}) - 1)}$ mod (prime number p).

24. (Previously presented) The system of claim 22, wherein the processor is further configured or arranged for performing the modulo operation if computation of a discrete logarithm is not possible.

25. (Currently amended) A machine-readable medium having program code stored thereon which, when executed by a machine, causes the machine to perform a method for selecting a digital object in a database, the method comprising:

generating a plurality of encryption keys, each encryption key associated with one of a plurality of digital objects stored in an electronic database;

encrypting the plurality of digital objects using the associated encryption keys;

encrypting the plurality of encryption keys by the database ~~using a first cryptography scheme~~;

transmitting to a requester the plurality of encrypted digital objects and encryption keys;

receiving from the requester at least one of the encryption keys, wherein the received encryption key has been ~~further encrypted using a second cryptography scheme~~ re-encrypted by the requester;

generating a partially decrypted encryption key at the database by decrypting the received encryption key ~~using the first cryptography scheme~~; and

transmitting the partially decrypted encryption key to the requester.

26. (Previously Presented) The machine-readable medium of claim 25, wherein the method further comprises encrypting the plurality of encryption keys by determining $(\text{encryption key})^{(\text{random number R})} \bmod (\text{prime number p})$ for each key.

27. (Currently amended) The machine-readable medium of claim 25, wherein the method further comprises decrypting the received encryption key by determining ~~$(\text{encryption key})^{(1/(\text{random number R}) \bmod (\text{prime number p} - 1))} \bmod (\text{prime number p})$~~ $(\text{encryption key})^{(1/(\text{random number R}) \bmod (\text{prime number p}) - 1)} \bmod (\text{prime number p})$.

28. (Previously presented) The machine-readable medium of claim 26, wherein the modulo operation is performed if computation of a discrete logarithm is not possible.

29. (Currently amended) A machine-readable medium having program code stored thereon which, when executed by a machine, causes the machine to perform a method for selecting a digital object in a database, the method comprising:

requesting a plurality of digital objects from an electronic database;

receiving from the database the requested plurality of digital objects, wherein each digital object has been encrypted using an associated encryption key;

receiving from the database the plurality of keys associated with the plurality of digital objects wherein each key has been encrypted ~~using a first cryptography scheme~~ by the database;

selecting a ciphertext key from the plurality of received keys;

~~further encrypting~~ re-encrypting the selected key ~~using a second cryptography scheme~~;

transmitting the further key to the database;

receiving from the database the key wherein the key has been partially decrypted ~~using the first cryptography scheme~~;

decrypting the partially decrypted key ~~using the second cryptography scheme~~ to generate a decrypted key; and

decrypting the received digital object using the decrypted key.

30. (Previously Presented) The machine-readable medium of claim 29, wherein the method further comprises encrypting the plurality of encryption keys by determining (encryption key)$^{(\text{random number R})}$ mod (prime number p) for each key.

31. (Currently amended) The machine-readable medium of claim 29, wherein the method further comprises decrypting the received encryption key by determining ~~(encryption key)$^{(1/(\text{random number R}) \bmod (\text{prime number p} - 1))}$ mod (prime number p)~~ (encryption key)$^{(1/(\text{random number R}) \bmod (\text{prime number p}) - 1)}$ mod (prime number p).

32. (Previously presented) The machine-readable medium of claim 27, wherein the method further comprises performing the modulo operation if computation of a discrete logarithm is not possible.